

WHAT IS CLAIMED IS:

1. An image data encryption method of encrypting image data, comprising:
 - a step of inputting image data, which is
 - 5 constituted by a plurality of data blocks, for each data block;
 - a determination step of determining whether the input data block is an object to be encrypted;
 - 10 an encryption step of encrypting the data block when it is determined in the determination step that the data block as the object to be encrypted is input;
 - 15 an addition step of adding terminating information to specify a terminating position of significant data for decoding to a start position of the data block encrypted in the encryption step;
 - a switching step of switching whether the addition step should be executed; and
 - an output step of outputting a data block which is determined in the determination step as a data block
 - 20 not to be encrypted and a data block generated via the switching step.
2. The method according to claim 1, further comprising a second addition step of adding the terminating information to an end position of the data block,
 - wherein the switching step switches between the addition step and the second addition step.

3. The method according to claim 2, wherein information representing whether the data block is encrypted is added immediately after the terminating information.
- 5 4. The method according to claim 1, wherein, in the terminating information addition step, the terminating information is replaced with the encrypted image data.
5. The method according to claim 1, wherein, in the determination step, it is determined whether the input 10 data block is an object which is set in advance as the object to be encrypted, and
 - in the switching step, switching is performed in accordance with setting information representing whether the encrypted data block should be transferred to decoding processing by the same procedures as that of an unencrypted data block.
- 15 6. The method according to claim 1, further comprising an encoding step of encoding (compressing) image data,
- 20 wherein in the input step, encoded (compressed) image data is input.
7. The method according to claim 6, wherein the encoding step comprises
 - a frequency conversion step of converting data in 25 a spatial domain into data in a frequency domain,
 - a quantization step of quantizing the data in the frequency domain and calculating a quantization index,

and

an entropy encoding step of entropy-encoding the quantization index.

8. The method according to claim 7, wherein the
5 entropy encoding step comprises

a region division step of dividing a predetermined frequency region into a plurality of rectangular regions which do not overlap each other,

an entropy encoding step of entropy-encoding the
10 quantization index for each bit plane in each rectangular region, and

an entropy codestream division step of dividing an entropy codestream in the rectangular region into at least a set of codestreams.

15 9. The method according to claim 8, wherein, in the addition step, the terminating information is added to each set of codestreams in the rectangular region.

10. The method according to claim 6, wherein the encoding step comprises

20 a frequency conversion step of converting data in a spatial domain into data in a frequency domain,

a quantization step of quantizing the data in the frequency domain and calculating a quantization index, and

25 an entropy encoding step of entropy-encoding the quantization index, and

in the encryption step, encryption processing is

executed for the entropy-encoded entropy codestream.

11. The method according to claim 6, wherein the
encoding step comprises

a frequency conversion step of converting data in

5 a spatial domain into data in a frequency domain,

a quantization step of quantizing the data in the
frequency domain and calculating a quantization index,
and

an entropy encoding step of entropy-encoding the
10 quantization index, and

in the encryption step, encryption processing is
executed for the quantized quantization index.

12. The method according to claim 6, wherein the
encoding step comprises

15 a frequency conversion step of converting data in
a spatial domain into data in a frequency domain,

a quantization step of quantizing the data in the
frequency domain and calculating a quantization index,
and

20 an entropy encoding step of entropy-encoding the
quantization index, and

in the encryption step, encryption processing is
executed for the frequency-converted data in the
frequency domain.

25 13. The method according to claim 10, wherein the
entropy encoding step comprises

a region division step of dividing a

predetermined frequency region into a plurality of rectangular regions which do not overlap each other,

an entropy encoding step of executing entropy-encoding for each bit plane in each rectangular region to generate an entropy codestream, and

5 an entropy codestream division step of dividing an entropy codestream in the rectangular region into at least a set of codestreams.

14. The method according to claim 13, wherein, in the 10 addition step, the terminating information is added to each set of codestreams in the rectangular region.

15. An image data conversion method of converting image data containing encrypted data for playback processing, comprising:

15 a step of inputting image data, which is constituted by a plurality of data blocks, for each data block;

a first determination step of determining whether the input data block is encrypted;

20 a second determination step of, when it is determined in the first determination step that the data block is encrypted, determining whether decryption key information is present;

a decryption step of, when it is determined in 25 the second determination step that the key information is present, decrypting the input data block in accordance with the key information and, when

terminating information to specify a terminating position of significant data is present at a start position of the decrypted data block, invalidating the terminating information; and

5 an output step of outputting the data block decrypted in the decryption step, a data block which is determined in the first determination step as an unencrypted data block, and a data block for which it is determined in the second determination step that no
10 key information is present.

16. The method according to claim 15, wherein invalidation of the terminating information in the decryption step is done by deleting the terminating information or placing the terminating information at
15 an end of the decrypted data block.

17. An image data conversion method of converting image data containing encrypted data for playback processing, comprising:

20 a step of inputting image data, which is constituted by a plurality of data blocks, for each data block;

 a first determination step of determining whether the input data block is encrypted;

25 a second determination step of, when it is determined in the first determination step that the data block is encrypted, determining whether decryption key information is present;

- a third determination step of, when it is determined in the second determination step that the key information is not present, and terminating information to specify a terminating position of
- 5 significant data is present at a start position of the input data block, determining whether the terminating information should be invalidated;
- a terminating information invalidation step of, when it is determined in the third determination step
- 10 that the terminating information should be invalidated, removing the terminating information or placing the terminating information at an end of the data block;
- a decryption step of, when it is determined in the second determination step that the key information
- 15 is present, decrypting the input data block; and
- an output step of outputting a data block which is determined in the first determination step as an unencrypted data block, a data block for which it is determined in the third determination step that the
- 20 terminating information should not be invalidated, a data block whose terminating information is invalidated in the terminating information invalidation step, and the data block decrypted in the decryption step.
18. The method according to claim 15, wherein the
- 25 image data input in the input step is encoded (compressed).
19. The method according to claim 18, further

comprising a decoding (decompression) step of decoding (decompressing) the encoded (compressed) data block output in the output step.

20. An image data encryption apparatus for encrypting
5 image data, comprising:

input means for inputting image data, which is constituted by a plurality of data blocks, for each data block;

10 determination means for determining whether the input data block is an object to be encrypted;

encryption means for encrypting the data block when said determination means determines that the data block as the object to be encrypted is input;

15 addition means for adding terminating information to specify a terminating position of significant data for decoding to a start position of the data block encrypted by said encryption means;

switching means for switching whether said addition means should be executed; and

20 output means for outputting a data block which is determined by said determination means as a data block not to be encrypted and a data block generated via said switching means.

21. An image data conversion apparatus for converting
25 image data containing encrypted data for playback processing, comprising:

input means for inputting image data, which is

constituted by a plurality of data blocks, for each data block;

first determination means for determining whether the input data block is encrypted;

5 second determination means for, when said first determination means determines that the data block is encrypted, determining whether decryption key information is present;

decryption means for, when said second 10 determination means determines that the key information is present, decrypting the input data block in accordance with the key information and, when terminating information to specify a terminating position of significant data is present at a start 15 position of the decrypted data block, invalidating the terminating information; and

output means for outputting the data block decrypted by said decryption means, a data block which is determined by said first determination step as an 20 unencrypted data block, and a data block for which it is determined by said second determination means that no key information is present.

22. An image data conversion apparatus for converting image data containing encrypted data for playback 25 processing, comprising:

input means for inputting image data, which is constituted by a plurality of data blocks, for each

data block;

first determination means for determining whether the input data block is encrypted;

second determination means for, when said first
5 determination means determines that the data block is encrypted, determining whether decryption key information is present;

third determination means for, when said second determination means determines that the key information
10 is not present, and terminating information to specify a terminating position of significant data is present at a start position of the input data block, determining whether the terminating information should be invalidated;

15 terminating information invalidation means for, when said third determination means determines that the terminating information should be invalidated, removing the terminating information or placing the terminating information at an end of the data block;

20 decryption means for, when said second determination means determines that the key information is present, decrypting the input data block; and

output means for outputting a data block which is determined by said first determination means as an
25 unencrypted data block, a data block for which it is determined by said third determination means that the terminating information should not be invalidated, a

data block whose terminating information is invalidated by said terminating information invalidation means, and the data block decrypted by said decryption means.

23. A computer program which functions as an image
5 data encryption apparatus for encrypting image data,
characterized by functioning as:

input means for inputting image data, which is constituted by a plurality of data blocks, for each data block;

- 10 determination means for determining whether the input data block is an object to be encrypted;

encryption means for encrypting the data block when said determination means determines that the data block as the object to be encrypted is input;

- 15 addition means for adding terminating information to specify a terminating position of significant data for decoding to a start position of the data block encrypted by said encryption means;

- switching means for switching whether said
20 addition means should be executed; and

output means for outputting a data block which is determined by said determination means as a data block not to be encrypted and a data block generated via said switching means.

- 25 24. A computer program which functions as an image data conversion apparatus for converting image data containing encrypted data for playback processing,

characterized by functioning as:

input means for inputting image data, which is constituted by a plurality of data blocks, for each data block;

5 first determination means for determining whether the input data block is encrypted;

second determination means for, when said first determination means determines that the data block is encrypted, determining whether decryption key

10 information is present;

decryption means for, when said second determination means determines that the key information is present, decrypting the input data block in accordance with the key information and, when

15 terminating information to specify a terminating position of significant data is present at a start position of the decrypted data block, invalidating the terminating information; and

output means for outputting the data block
20 decrypted by said decryption means, a data block which is determined by said first determination step as an unencrypted data block, and a data block for which it is determined by said second determination means that no key information is present.

25 25. A computer program which functions as an image data conversion apparatus for converting image data containing encrypted data for playback processing,

characterized by functioning as:

input means for inputting image data, which is constituted by a plurality of data blocks, for each data block;

5 first determination means for determining whether the input data block is encrypted;

second determination means for, when said first determination means determines that the data block is encrypted, determining whether decryption key

10 information is present;

third determination means for, when said second determination means determines that the key information is not present, and terminating information to specify a terminating position of significant data is present
15 at a start position of the input data block,
determining whether the terminating information should be invalidated;

terminating information invalidation means for, when said third determination means determines that the
20 terminating information should be invalidated, removing the terminating information or placing the terminating information at an end of the data block;

decryption means for, when said second determination means determines that the key information
25 is present, decrypting the input data block; and

output means for outputting a data block which is determined by said first determination means as an

- unencrypted data block, a data block for which it is determined by said third determination means that the terminating information should not be invalidated, a data block whose terminating information is invalidated 5 by said terminating information invalidation means, and the data block decrypted by said decryption means.
26. A computer-readable storage medium characterized by storing a computer program of claim 23.
27. A computer-readable storage medium characterized 10 by storing a computer program of claim 24.
28. A computer-readable storage medium characterized by storing a computer program of claim 25.